Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 26 avril 2002
N° CERTA-2002-AVI-088

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de sudo

Gestion du document

Référence	CERTA-2002-AVI-088
Titre	Vulnérabilité de sudo
Date de la première version	26 avril 2002
Date de la dernière version	–
Source(s)	Avis de sécurité Red Hat RHSA-2002:072-07 Avis de sécurité Mandrake MDKSA-2002:028 Avis de sécurité Debian DSA-128-1
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Elévation de privilèges.

2 Systèmes affectés

Sudo versions 1.6.5 et antérieures.

3 Résumé

Un utilisateur mal intentionné peut exploiter une vulnérabilité de la commande *sudo* pour obtenir les droits de l'administrateur *root*.

4 Description

La commande *sudo* permet de donner les droits de l'administrateur *root* à certains utilisateurs du système pour exécuter certaines commandes particulières.

Il est possible d'exécuter la commande *sudo* avec l'option *-p*, pour spécifier le *prompt* de mot passe devant être affiché. En choisissant habilement le paramètre de cette option, un utilisateur local mal intentionné peut provoquer un débordement de mémoire qui peut être exploité pour exécuter du code arbitraire avec les droits de l'administrateur.

5 Contournement provisoire

Retirer le bit *suid* de la commande */usr/bin/sudo*.

6 Solution

Installer la version 1.6.6 disponible sur le site de *Sudo*, ou appliquer le correctif de votre éditeur.

7 Documentation

- Site de *Sudo* :
  http://www.sudo.ws
- Bulletin de sécurité Red Hat RHSA-2002:072-07 :
  http://www.redhat.com/apps/support/errata/
- Bulletin de sécurité Mandrake MDKSA-2002:028 :
  http://www.linux-mandrake.com/en/security/
- Bulletin de sécurité Debian DSA-128-1 :
  http://www.debian.org/security/

Gestion détaillée du document

26 avril 2002 version initiale.